

Subfield-Subcodes of Generalized Toric codes

Fernando Hernando, Michael E. O'Sullivan,
Emanuel Popovici and Shraddha Srivastava*

Abstract

We study subfield-subcodes of Generalized Toric (GT) codes over \mathbb{F}_{p^s} . These are the multidimensional analogues of BCH codes, which may be seen as subfield-subcodes of generalized Reed-Solomon codes [2], [3], [6], [10], [11]. We identify polynomial generators for subfield-subcodes of GT codes which allows us to determine the dimensions and obtain bounds for the minimum distance. We give several examples of binary and ternary subfield-subcodes of GT codes that are the best known codes of a given dimension and length.

1 Generalized Toric codes

Toric codes are algebraic geometry codes over toric varieties. These codes were introduced by J.P. Hansen [4], see also [5], [7]. Let M be an integral lattice and P be a convex polytope in $M \otimes \mathbb{R}$. The toric code C_P over \mathbb{F}_q associated to P is the evaluation code generated by the monomials x^α where $\alpha \in P \cap M$ at the points of the algebraic torus $T = (\mathbb{F}_q^*)^r$. A lower bound for the minimum distance is estimated in [9] using intersection theory and mixed volumes, extending the methods of J.P. Hansen for plane polytopes.

D.Ruano introduces a natural generalization of this family, the so called Generalized Toric Codes [8], which consist of the evaluation of any polynomial algebra in the algebraic torus. More precisely, one may consider any subset $U \subseteq \{0, \dots, q-2\}^r$ and the corresponding vector space $\mathbb{F}_q[U] = \langle \{x^u = x_1^{u_1} \cdots x_r^{u_r} \mid u = (u_1, \dots, u_r) \in U\} \rangle \subset \mathbb{F}_q[x_1, \dots, x_r]$, thus the Generalized toric code, C_U , is the image under the \mathbb{F}_q -linear map, $ev : \mathbb{F}_q[U] \rightarrow \mathbb{F}_q^n$, $ev(f) = (f(t))_{t \in T}$, $n = (q-1)^r$. It is clear from his construction that any toric code is a GT code.

Proposition 1.1. *Let $H = \{0, \dots, q-2\}^r$ and $n = (q-1)^r$. The \mathbb{F}_q -linear map*

$$ev : \mathbb{F}_q[H] \rightarrow \mathbb{F}_q^n, \quad f \mapsto (f(t))_{t \in T}$$

is an isomorphism

*This work is supported by Science Foundation Ireland (SFI) Claude Shannon Institute, grant number 06/MI/006. F.Hernando is also partially supported by MEC MTM2007-64704 and Junta de CyL VA025A07 (Spain). M. E. O'Sullivan is supported by the National Science Foundation under Grant No. CCF-0916492.

Corollary 1.2. *In particular, ev restricted to $\mathbb{F}_q[U]$ is injective, so $\dim(C_U) = |U|$*

The next result may be found in [1] and [8].

Proposition 1.3. *For $u \in H$, let $\hat{u} \in H$ be defined by $\hat{u}_i = 0$ if $u_i = 0$ and $\hat{u}_i = q - 1 - u_i$ if $u_i \neq 0$. Let C be the GT code defined by $U \subset H$, then C^\perp is the GT code defined by $U^\perp = \{\hat{u} : u \in U\}$.*

2 Subfield-Subcodes

From now on $q = p^s$ where p is a prime number.

Definition 2.1. *Let C be a linear code of length n over \mathbb{F}_{p^s} , the subfield-subcode of C , say D , is the set of the codewords $c \in C$ such that $c \in \mathbb{F}_p^n$, i.e., $D = C \cap \mathbb{F}_p^n$.*

Many authors have been interested in computing the dimension of subfield-subcodes. Delsarte studied in [3] the subfield-subcodes of modified Reed-Solomon codes. Stichtenoth improved this lower bound in [11] and Shibuya et al gave a better lower bound [10]. Later on Hattori, McEliece and Solomon gave a lower bound on the dimension of subspace-subcodes of Reed-Solomon codes. Finally Jie and Junying generalize the previous bound for Generalized Reed-Solomon codes.

In particular Delsarte provides the following result [3]:

Theorem 2.2.

$$(C \cap \mathbb{F}_p^n)^\perp = \text{Tr}(C^\perp)$$

where $\text{Tr} : \mathbb{F}_{p^s} \rightarrow \mathbb{F}_p$ sending x to $x + x^p + \dots + x^{p^{s-1}}$.

The next result is provided in [12] although it is possibly known before.

Proposition 2.3. *A BCH code D over \mathbb{F}_p of length $n = p^s - 1$ is a subfield-subcode of a Reed-Solomon code C over \mathbb{F}_{p^s} , and therefore $d(D) \geq d(C)$.*

3 Subfield subcodes of Generalized Toric codes

Let R be $\mathbb{F}_{p^s}[y_1, \dots, y_r] / \langle y_1^{p^s-1} - 1, \dots, y_r^{p^s-1} - 1 \rangle$. We are looking for $f \in R$ such that $f(t) \in \mathbb{F}_p, \forall t \in T$. If this occurs we say that f is a polynomial evaluating to \mathbb{F}_p . The idea is to find out first all those polynomials evaluating to \mathbb{F}_p in R and then restrict this set to $\mathbb{F}_{p^s}[U]$.

Proposition 3.1. $ev(f) \in \mathbb{F}_p^n \Leftrightarrow f(t) = (f(t))^p \forall t \in T \Leftrightarrow f^p = f$ in R .

Proof. According to Proposition 1.1 we know that $ev(f)^p = ev(f^p)$ then it is clear that:

$$\begin{aligned} ev(f) \in \mathbb{F}_p^n &\Leftrightarrow f(t) = (f(t))^p \forall t \in T \Leftrightarrow ev(f) = ev(f)^p \Leftrightarrow ev(f) = ev(f^p) \Leftrightarrow \\ ev(f - f^p) &= 0 \Leftrightarrow f - f^p \in \ker(ev) \Leftrightarrow f^p(\underline{y}) = f(\underline{y}) \text{ in } R. \quad \square \end{aligned}$$

Consider $G = \text{Gal}(\mathbb{F}_{p^s} \mid \mathbb{F}_p) = \{g_0, \dots, g_{s-1}\}$ the Galois group, where g_i maps α to α^{p^i} . Looking at exponents, we may consider G to act on \mathbb{Z}_{p^s-1} by multiplying by p and this may be naturally extended to $\mathbb{Z}_{p^s-1} \times \dots \times \mathbb{Z}_{p^s-1}$ by multiplying by p coordinate wise. The orbits of G on $\mathbb{Z}_{p^s-1} \times \dots \times \mathbb{Z}_{p^s-1}$ are called cyclotomic cosets, i.e., for every $\underline{b} \in (\mathbb{Z}_{p^s-1})^r$ we define the cyclotomic coset $I_{\underline{b}}$ by $\{\underline{b}, p\underline{b}, \dots, p^{n_{\underline{b}}-1}\underline{b}\}$ where $n_{\underline{b}}$ is the smallest positive integer such that $\underline{b} = \underline{b}p^{n_{\underline{b}}}$. The integer $n_{\underline{b}}$ is the cardinal of $I_{\underline{b}}$.

Some known properties of cyclotomic cosets:

Proposition 3.2.

- (i) $I_{\underline{b}} = \{\underline{b}, p\underline{b}, p^2\underline{b}, \dots, p^{n_{\underline{b}}-1}\underline{b}\}$ is closed under multiplication by p .
- (ii) The cardinal of $I_{\underline{b}}$ is either s or a divisor of it.
- (iii) $I_{\underline{b}}$ and $I_{\underline{b}'}$ are either identical or they don't intersect. Thus $\mathcal{B} = \{I_{\underline{b}} : \underline{b} \in (\mathbb{Z}_{p^s-1})^r\}$ partitions $(\mathbb{Z}_{p^s-1})^r$.

If $\theta : R \rightarrow R$ is an isomorphism and f evaluates to \mathbb{F}_p . Then so does $\theta(f)$. This is because $\theta(f)^p = \theta(f^p) = \theta(f)$. So it is worthwhile cataloguing some isomorphisms of R .

Proposition 3.3. (i) For any i coprime with $p^s - 1$, the map θ_i fixing \mathbb{F}_{p^s} and taking $f(y_1, \dots, y_r) \rightarrow f(y_1^i, \dots, y_r^i)$ is an isomorphism of R .

(ii) For any $\underline{\alpha} \in \mathbb{F}_{p^s}^* \times \dots \times \mathbb{F}_{p^s}^*$, the map $\theta_{\underline{\alpha}}$ fixing \mathbb{F}_{p^s} and taking $f(y_1, \dots, y_r) \rightarrow f(\alpha_1 y_1, \dots, \alpha_r y_r)$ is an isomorphism of R .

(iii) The Frobenius map on \mathbb{F}_{p^s} combined with $y_i \mapsto y_i$ for $i = 1, \dots, r$.

Let $f(\underline{y}) = \sum a_{i_1, \dots, i_r} y_1^{i_1} \dots y_r^{i_r} \in R$, we denote $\text{supp}(f) = \{\underline{i} \mid a_{\underline{i}} \neq 0\}$ as the support of f . If $I_{\underline{b}}$ is a cyclotomic coset, we denote $f_{I_{\underline{b}}} = \sum_{\underline{i} \in I_{\underline{b}}} a_{\underline{i}} y_1^{i_1} \dots y_r^{i_r}$ as the polynomial having $\text{supp}(f) = I_{\underline{b}}$ and coefficients equal to one.

It is easy to verify that $f_{I_{\underline{b}}}$ evaluates to \mathbb{F}_p . Note that $\theta_{\underline{\alpha}}(f_{I_{\underline{b}}}) = \sum_{\underline{i} \in I_{\underline{b}}} \alpha_1^{i_1} y_1^{i_1} \dots \alpha_r^{i_r} y_r^{i_r}$ is the polynomial with support $I_{\underline{b}}$ and coefficients determined by $\underline{\alpha}$. Since $\theta_{\underline{\alpha}}$ is an isomorphism, $\theta_{\underline{\alpha}}(f_{I_{\underline{b}}})$ evaluates to \mathbb{F}_p .

Let $l = |\mathcal{B}|$ be the number of cyclotomic cosets and let $J = \{\underline{b}_1, \dots, \underline{b}_l\}$, be a set of representatives, so $\mathcal{B} = \{I_{\underline{b}_1}, \dots, I_{\underline{b}_l}\}$. From now on we will denote by $f_{I_{\underline{b}}, \beta}$ the polynomial with support $I_{\underline{b}}$ and leading coefficient β , i.e., $f_{I_{\underline{b}}, \beta} = \beta \underline{y}^{\underline{b}} + \beta^p \underline{y}^{p\underline{b}} + \dots + \beta^{p^{n_{\underline{b}}-1}} \underline{y}^{p^{n_{\underline{b}}-1}\underline{b}}$. Note that $f_{I_{\underline{b}}, \beta}$ evaluates to \mathbb{F}_p if and only if $\beta \in \mathbb{F}_{p^{n_{\underline{b}}}}$.

Proposition 3.4. Let f be a function that evaluates to \mathbb{F}_p with $\text{supp}(f) = I_{\underline{b}}$ and let β be a primitive element of $\mathbb{F}_{p^{n_{\underline{b}}}}$. Then, f is a linear combination of $f_{I_{\underline{b}}}, f_{I_{\underline{b}}, \beta}, \dots, f_{I_{\underline{b}}, \beta^{n_{\underline{b}}-1}}$.

Proof. Since $\text{supp}(f) = I_{\underline{b}}$ and $f^p = f$ there is some α such that $f = \alpha \underline{y}^{\underline{b}} + \alpha^p \underline{y}^{p\underline{b}} + \dots + \alpha^{p^{n_{\underline{b}}-1}} \underline{y}^{p^{n_{\underline{b}}-1}\underline{b}}$. Moreover $\alpha^{p^{n_{\underline{b}}}} = \alpha$, which implies that $\alpha \in \mathbb{F}_{p^{n_{\underline{b}}}}$.

We know that $\{1, \beta, \dots, \beta^{(n_{\underline{b}}-1)}\}$ is a basis of $\mathbb{F}_p^{n_{\underline{b}}}$ over \mathbb{F}_p , so $\alpha = a_0 + a_1\beta + \dots + a_{n_{\underline{b}}-1}\beta^{(n_{\underline{b}}-1)}$, with $a_i \in \mathbb{F}_p$ for all i . Therefore,

$$\begin{aligned} f &= \sum_{i=0}^{n_{\underline{b}}-1} \alpha^{p^i} \underline{y}^{bp^i} = \sum_{i=0}^{n_{\underline{b}}-1} \underline{y}^{bp^i} \left(\sum_{j=0}^{n_{\underline{b}}-1} a_j \beta^j \right)^{p^i} \\ &= \sum_{j=0}^{n_{\underline{b}}-1} a_j \sum_{i=0}^{n_{\underline{b}}-1} \beta^{jp^i} \underline{y}^{bp^i} = \sum_{j=0}^{n_{\underline{b}}-1} a_j f_{I_{\underline{b}}, \beta^j} \end{aligned}$$

□

Proposition 3.5. $f_{I_{\underline{b}}}, f_{I_{\underline{b}}, \beta}, \dots, f_{I_{\underline{b}}, \beta^{n_{\underline{b}}-1}}$ are linearly independent over \mathbb{F}_p .

Proof. Suppose it is not true. Thus, $a_0 f_{I_{\underline{b}}} + a_1 f_{I_{\underline{b}}, \beta} + \dots + a_{n_{\underline{b}}-1} f_{I_{\underline{b}}, \beta^{n_{\underline{b}}-1}} = 0$. The smallest monomial in the left hand side is $(a_0 + a_1\beta + \dots + a_{n_{\underline{b}}-1}\beta^{(n_{\underline{b}}-1)})\underline{y}^{\underline{b}}$ which has to be zero. This is true if β is a root of $p(z) = a_0 + a_1z + \dots + a_{n_{\underline{b}}-1}z^{n_{\underline{b}}-1}$, but this is not possible because the minimal polynomial of β has degree $n_{\underline{b}}$. □

Theorem 3.6. A basis for the set of polynomials evaluating to \mathbb{F}_p is:

$$\bigcup_{I_{\underline{b}} \in \mathcal{B}} \{f_{I_{\underline{b}}, \beta^j} : j \in \{0, \dots, n_{\underline{b}}-1\}, \beta \text{ primitive in } \mathbb{F}_p^{n_{\underline{b}}}\}.$$

Proof. If $I_{\underline{b}}$ and $I_{\underline{b}'}$ are two different cosets then $f_{I_{\underline{b}}, \beta}$ and $f_{I_{\underline{b}'}, \beta'}$ have different degrees. So, there is no way to generate one from the other which proves that different classes are linearly independent. Moreover within the set of polynomials with the same support, say $I_{\underline{b}}$, we know from Corollary 3.5 that the only linearly independent are $\{f_{I_{\underline{b}}, 1}, f_{I_{\underline{b}}, \beta}, \dots, f_{I_{\underline{b}}, \beta^{n_{\underline{b}}-1}}\}$. So, the only part left is to see that it is a system of generators.

Consider the smallest monomial in f , say $\beta^{j_1} \underline{y}^{\underline{b}}$ then $f_{I_{\underline{b}}, \beta^{j_1}} = \sum_{k=0}^{n_{\underline{b}}-1} (\beta^{j_1} \underline{y}^{\underline{b}})^{p^k}$ must appear in f . Since $\beta^{j_1} \underline{y}^{\underline{b}}$ is the smallest monomial in f , therefore \underline{b} must be one of the leaders in $J = \{\underline{b}_1, \dots, \underline{b}_l\}$. Assume without loss of generality that $\underline{b}_1 < \underline{b}_2 < \dots < \underline{b}_l$ and $\underline{b} = \underline{b}_1$.

Consider $f_1 = f - f_{I_{\underline{b}_1}, \beta^{j_1}}$ and the first monomial on it, say $\beta^{j_2} \underline{y}^{\underline{b}'}$. Again, the polynomial $f_{I_{\underline{b}'}, \beta^{j_2}} = \sum_{k=0}^{n_{\underline{b}}-1} (\beta^{j_2} \underline{y}^{\underline{b}'})^{p^k}$ must appear in f_1 . We may assume that $\underline{b}' = \underline{b}_2$ and consider $f_2 = f_1 - f_{I_{\underline{b}_2}, \beta^{j_2}}$.

In at most l -steps, we can finish the process obtaining that $f = a_1 f_{I_{\underline{b}_1}, \beta^{j_1}} + \dots + a_l f_{I_{\underline{b}_l}, \beta^{j_l}}$, which concludes the proof. □

For the next result we introduce an \mathbb{F}_p linear mapping on R extending the trace map, $T : R \rightarrow R$ is given by $g \mapsto g + g^p + \dots + g^{p^{s-1}}$ for all $g \in R$.

Corollary 3.7. The image of T is exactly the set of $f \in R$ that evaluate to \mathbb{F}_p .

Proof. Let $f = T(g) = g + g^p + \dots + g^{p^{s-1}}$. Since $g^{p^s} = g$ in R we have $f^p = f$. Thus any image of the map T evaluates to \mathbb{F}_p .

For the converse, it is sufficient, by Proposition 3.4, to show that each $f_{I_{\underline{b}}, \beta}$ is in the image of T for β an element of $\mathbb{F}_{p^{n_{\underline{b}}}}$. Let $\gamma \in \mathbb{F}_{p^s}$ be such that $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_{p^{n_{\underline{b}}}}}(\gamma) = \beta$. Then

$$\begin{aligned} T(\gamma \underline{y}^{\underline{b}}) &= \sum_{i=0}^{s-1} \gamma^{p^i} \underline{y}^{b p^i} \\ &= \sum_{j=0}^{\frac{s}{n_{\underline{b}}}-1} \sum_{i=0}^{n_{\underline{b}}-1} \gamma^{p^{i+j n_{\underline{b}}}} \underline{y}^{b p^{i+j n_{\underline{b}}}} \end{aligned}$$

Since $b p^{n_{\underline{b}}} = b$,

$$= \sum_{i=0}^{n_{\underline{b}}-1} \underline{y}^{b p^i} \left(\sum_{j=0}^{\frac{s}{n_{\underline{b}}}-1} \gamma^{(p^{n_{\underline{b}}})^j} \right)^{p^i}$$

The term in parentheses is $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_{p^{n_{\underline{b}}}}}(\gamma) = \beta$, so

$$T(\gamma \underline{y}^{\underline{b}}) = f_{I_{\underline{b}}, \beta}$$

□

This provides us a constructive way of producing all those polynomials which evaluate to \mathbb{F}_p . In particular, if we restrict to those polynomials with support in U , we trivially have a formula for the dimension of a subfield-subcode.

Theorem 3.8. *Let $U \subseteq \{0, \dots, q-2\}^r$ and let $D_U = C_U \cap \mathbb{F}_p^n$.*

$$D_U = \text{ev} \left(T(\mathbb{F}_{p^s}[H]) \cap \mathbb{F}_{p^s}[U] \right)$$

A basis for D_U is:

$$\bigcup_{I_{\underline{b}}: I_{\underline{b}} \subseteq U} \{f_{I_{\underline{b}}, \beta^j} : j \in \{0, \dots, n_{\underline{b}}-1\}, \beta \text{ primitive in } \mathbb{F}_{p^{n_{\underline{b}}}}\}$$

Moreover it has dimension

$$\dim D_U = \sum_{I_{\underline{b}}: I_{\underline{b}} \subseteq U} n_{\underline{b}}$$

.

Remark 3.1. When $r = 1$ and $U = \{0, 1, 2, \dots, k-1\}$ the GT code is a Reed-Solomon code with parameters $[p^s - 1, k, p^s - k]$.

Example 3.9. Let C be an $[n, k, d]$ Reed-Solomon code with $q = 2^4$, $n = 15$, i.e. we evaluate all the polynomials of degree less than or equal to $k - 1$, at all the points of \mathbb{F}_{16}^* . Let D be the subfield-subcode of C , that is, $D = C \cap \mathbb{F}_2^{15}$. What are the functions $f : \mathbb{F}_{16} \rightarrow \mathbb{F}_2$ we have to evaluate to get D ?

The different cosets are $I_0 = \{0\}$, $I_1 = \{1, 2, 4, 8\}$, $I_3 = \{3, 6, 12, 9\}$, $I_5 = \{5, 10\}$, $I_7 = \{7, 14, 13, 11\}$. Depending on the value of k we have:

- From $1 \leq k \leq 8$, the only function is $f = 1$ corresponding to the coset I_0 , so the code D is $[15, 1, 15]$.
- If $k = 9$, $C = [15, 9, 7]$ then we have $T_r(x) = f_{I_1}, f_{I_1, \alpha}, f_{I_1, \alpha^2}, f_{I_1, \alpha^3}$ and $f_{I_0} = 1$. Then D is a $[15, 5, 7]$ code.
- If $k = 10$ nothing new.
- If $k = 11$, $C = [15, 11, 5]$ we consider I_0, I_1 and I_5 . That is $f_{I_5} = x^5 + x^{10}$ and $f_{I_1, \alpha} = \alpha^5 x^5 + \alpha^{10} x^{10}$ in addition to the previous functions. Therefore, $D = [15, 7, 5]$.
- If $k = 12$ nothing new.
- If $k = 13$, $C = [15, 13, 3]$ we consider I_0, I_1, I_5 and I_3 . That is $f_{I_3, \alpha^i} = \alpha^{3i} x^3 + \alpha^{6i} x^6 + \alpha^{9i} x^9 + \alpha^{12i} x^{12}$ in addition to the previous functions, for $0 \leq i \leq 3$. Therefore, $D = [15, 11, 3]$.
- If $k = 14$ nothing new.
- If $k = 15$, $C = [15, 15, 1]$ and $D = [15, 15, 1]$ with the 4 new functions corresponding to I_7 : $f_{I_7, \alpha^i} = \alpha^{7i} x^7 + \alpha^{11i} x^{11} + \alpha^{13i} x^{13} + \alpha^{14i} x^{14}$ for $0 \leq i \leq 3$.

4 Dual of Subfield-Subcodes

Theorem 2.2 together with Theorem 3.8 motivate this section.

Let $U \subseteq \{0, \dots, q - 2\}^r$ and let $C_U = \text{ev}(\mathbb{F}_{p^s}[U])$ and $D_U = C_U \cap \mathbb{F}_p^n$. From Proposition 1.3, we know that C_U^\perp is the GT code defined by U^\perp . From Delsarte's Theorem we have

$$D_U^\perp = \text{Tr}(C_{U^\perp}) = \text{Tr}(\text{ev}(\mathbb{F}_{p^s}[U^\perp])) = \text{ev}(T(\mathbb{F}_{p^s}[U^\perp]))$$

The last equality follows from $\text{ev} \circ T = \text{Tr} \circ \text{ev}$, which is easily verified. Clearly, $T(\mathbb{F}_{p^s}[U^\perp])$ is spanned by $T(\gamma y^{\underline{b}})$ for $\underline{b} \in U^\perp$ and $\gamma \in \mathbb{F}_{p^s}$. For \underline{b} fixed and varying γ we get exactly the set of $f_{I_{\underline{b}}, \beta}$ for $\beta \in \mathbb{F}_{p^{n_{\underline{b}}}}$. Thus we have a basis for D_U^\perp .

Theorem 4.1. D_U^\perp has the basis

$$\bigcup_{I_{\underline{b}} \cap U^\perp \neq \emptyset} \{f_{I_{\underline{b}}, \beta^j} : j \in \{0, \dots, n_{\underline{b}} - 1\}, \beta \text{ primitive in } \mathbb{F}_{p^{n_{\underline{b}}}}\}$$

We therefore have

$$\dim D_U^\perp = \sum_{I_{\underline{b}}: I_{\underline{b}} \cap U^\perp \neq \emptyset} n_{\underline{b}}.$$

Proposition 4.2. *Let $\hat{U} = \{\text{supp}(h) \mid h = \text{Tr}(\underline{y}^{\underline{b}}), \underline{b} \in U^\perp\} = \{I_{\underline{b}} \mid \underline{b} \in U^\perp\} = \{p^i \underline{b} \mid \underline{b} \in U^\perp, i = 0, 1, \dots, n_{\underline{b}} - 1\}$. Then $D_U^\perp = C_{\hat{U}} \cap \mathbb{F}_p^n = D_{\hat{U}}$.*

Corollary 4.3. *One can always decode D^\perp up to $t = \lfloor d(C_{\hat{U}}) - 1/2 \rfloor$ with the decoding algorithm for $C_{\hat{U}}$.*

5 Computations

From the practical point of view it makes sense to choose U to be the union of different cyclotomic cosets, otherwise the evaluation will not be in \mathbb{F}_p^n .

We have written a Magma function for computing the subfield-subcode of a GT code and we have found a number of optimal codes. Consider first the field $GF(2^3)$ and $r = 2$ so T is the toric surface. In each of the following cases we give a subset U of $(\mathbb{Z}_7)^2$ and the parameters of $D = D_U$ and $D^\perp = D_U^\perp$, the subfield-subcode of C_U and its dual.

- i) $U = [[1, 0], [2, 0], [4, 0], [0, 1], [0, 2], [0, 4]]$.
 D is $[49, 6, 24]$ and D^\perp is $[49, 43, 3]$.
- ii) $U = [[6, 3], [5, 6], [3, 5], [3, 1], [6, 2], [5, 4], [6, 1], [5, 2], [3, 4]]$.
 D is $[49, 9, 20]$ and D^\perp is $[49, 39, 3]$.
- iii) $U = [[2, 1], [4, 2], [1, 4], [3, 1], [6, 2], [5, 4], [4, 1], [1, 2], [2, 4], [0, 0]]$.
 D is $[49, 10, 20]$ and D^\perp is $[49, 39, 4]$. If we consider $U' = U \cup \{[1, 0], [2, 0], [5, 0], [6, 0], [1, 1], [2, 2]\}$ we get a new toric code, $C_{U'}$, with parameters $[49, 16, 18]$, i.e, the minimum distance drops by 2 (with respect to C_U) and the subfield-subcode $D_{U'}$ is equal to D_U . The previous is an example of a subfield-subcode $D_{U'}$ of a GT code $C_{U'}$ where $d(D_{U'}) > d(C_{U'})$.
- iv) $U = [[1, 0], [2, 0], [4, 0], [2, 3], [4, 6], [1, 5], [0, 1], [0, 2], [0, 4], [6, 3], [5, 6], [3, 5], [6, 1], [5, 2], [3, 4]]$.
 D is $[49, 15, 16]$ and D^\perp is $[49, 34, 6]$.
- v) $U = [[1, 0], [2, 0], [4, 0], [0, 1], [0, 2], [0, 4], [1, 1], [2, 2], [4, 4], [2, 1], [4, 2], [1, 4], [3, 1], [6, 2], [5, 4], [4, 1], [1, 2], [2, 4], [1, 3], [2, 6], [4, 5]]$.
 D is $[49, 21, 12]$ and D^\perp is $[49, 28, 7]$. We use again the same strategy of adding points: consider $U' = U \cup \{[3, 0], [6, 0], [6, 1], [5, 2]\}$, we obtain the GT code $C_{U'}$ with parameters $[49, 25, 9]$ where the minimum distance drops by 3 and the subfield-subcode $D_U = D_{U'}$.

- vi) $U = [[6, 3], [5, 6], [3, 5], [1, 0], [2, 0], [4, 0], [3, 0], [6, 0], [5, 0], [2, 1], [4, 2], [1, 4], [3, 1], [6, 2], [5, 4], [4, 1], [1, 2], [2, 4], [5, 1], [3, 2], [6, 4], [1, 3], [2, 6], [4, 5], [2, 3], [4, 6], [1, 5], [3, 3], [6, 6], [5, 5], [4, 3], [1, 6], [2, 5]]$.
 D is $[49, 33, 6]$ and D^\perp is $[49, 16, 7]$.
- vii) $U = [[6, 3], [5, 6], [3, 5], [0, 0], [0, 1], [0, 2], [0, 4], [1, 1], [2, 2], [4, 4], [3, 1], [6, 2], [5, 4], [5, 1], [3, 2], [6, 4], [6, 1], [5, 2], [3, 4], [0, 3], [0, 6], [0, 5], [2, 3], [4, 6], [1, 5], [3, 3], [6, 6], [5, 5], [4, 3], [1, 6], [2, 5], [5, 3], [3, 6], [6, 5]]$.
 D is $[49, 34, 6]$ and D^\perp is $[49, 15, 12]$.
- viii) $U = [[6, 3], [5, 6], [3, 5], [0, 0], [1, 0], [2, 0], [4, 0], [3, 0], [6, 0], [5, 0], [1, 1], [2, 2], [4, 4], [2, 1], [4, 2], [1, 4], [4, 1], [1, 2], [2, 4], [5, 1], [3, 2], [6, 4], [6, 1], [5, 2], [3, 4], [0, 3], [0, 6], [0, 5], [1, 3], [2, 6], [4, 5], [3, 3], [6, 6], [5, 5], [4, 3], [1, 6], [2, 5], [5, 3], [3, 6], [6, 5]]$.
 D is $[49, 40, 4]$ and D^\perp is $[49, 9, 14]$.
- ix) $U = [[0, 0], [1, 0], [2, 0], [4, 0], [3, 0], [6, 0], [5, 0], [0, 1], [0, 2], [0, 4], [1, 1], [2, 2], [4, 4], [2, 1], [4, 2], [1, 4], [3, 1], [6, 2], [5, 4], [4, 1], [1, 2], [2, 4], [5, 1], [3, 2], [6, 4], [6, 1], [5, 2], [3, 4], [0, 3], [0, 6], [0, 5], [1, 3], [2, 6], [4, 5], [2, 3], [4, 6], [1, 5], [3, 3], [6, 6], [5, 5], [4, 3], [1, 6], [2, 5], [5, 3], [3, 6], [6, 5]]$.
 D is $[49, 46, 2]$ and D^\perp is $[49, 3, 28]$.

Notice that $p = 2 \nmid s = 3$ thus from Theorem 4.1 we know that the dual of a subfield-subcode is again the subfield-subcode of another toric code. In each example the code D is the best known code for a fixed length and dimension. Also in each example, except vi),vii) and viii) the dual code has the same correction capability as the best known code for a fixed length and dimension.

From now on we will denote by D the subfield-subcode of the GT codes over $GF(3^2)$ and $r = 2$. In each of the following cases we give a subset U of $(\mathbb{Z}_8)^2$ and the parameters of $D = D_U$ and $D^\perp = D_U^\perp$, the subfield-subcode of C_U and its dual.

- i) $U = [[5, 0], [7, 0], [5, 5], [7, 7]]$
 D is $[64, 4, 42]$ and D^\perp is $[64, 60, 2]$.
- ii) $U = [[5, 1], [7, 3], [0, 0], [0, 0], [7, 1], [5, 3], [1, 2], [3, 6], [2, 1], [6, 3]]$
 D is $[64, 9, 36]$ and D^\perp is $[64, 55, 4]$.
- iii) $U = [[7, 1], [5, 3], [5, 0], [7, 0], [0, 1], [0, 3], [1, 5], [3, 7], [2, 1], [6, 3], [6, 2], [2, 6]]$.
 D is $[64, 12, 30]$ and D^\perp is $[64, 52, 4]$.
- iv) $U = [[0, 0], [4, 0], [0, 4], [4, 4], [5, 0], [7, 0], [0, 1], [0, 3], [1, 1], [3, 3], [2, 1], [6, 3], [3, 1], [1, 3], [4, 1], [4, 3], [5, 1], [7, 3], [6, 1], [2, 3], [1, 2], [3, 6], [2, 2], [6, 6], [3, 2], [1, 6], [4, 2], [4, 6], [5, 2], [7, 6], [6, 2], [2, 6], [7, 2], [5, 6], [1, 4], [3, 4], [2, 4], [6, 4], [0, 5], [0, 7], [5, 4], [7, 4], [1, 5], [3, 7], [2, 5], [6, 7], [3, 5], [1, 7], [7, 5], [5, 7]]$
 D is $[64, 50, 5]$ and D^\perp is $[64, 14, 27]$. Consider $U' = U \cup \{[1, 0], [6, 0], [6, 5], [7, 7], [4, 7]\}$ the new GT code $C_{U'}$ has parameters $[64, 55, 4]$ where the minimum distance drops by 1 but $D_U = D_{U'}$.

In all the examples the code D has the same correction capability to the best known codes for a fixed length and dimension.

References

- [1] Bras-Amorós, Maria; O’Sullivan, Michael E. Duality for some families of correction capability optimized evaluation codes. *Adv. Math. Commun.* 2 (2008), no. 1, 15–33.
- [2] Cui, Jie; Pei, Junying. Subspace subcodes of generalized Reed-Solomon codes. *Acta Math. Appl. Sinica (English Ser.)* 17 (2001), no. 4, 503–508.
- [3] Delsarte, P. On subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Information Theory* IT-21 (1975), no. 5, 575–576.
- [4] Hansen, Johan P. Toric surfaces and error-correcting codes. *Coding theory, cryptography and related areas (Guanajuato, 1998)*, 132–142, Springer, Berlin, 2000.
- [5] Hansen, Johan P. Toric varieties Hirzebruch surfaces and error-correcting codes. *Appl. Algebra Engrg. Comm. Comput.* 13 (2002), no. 4, 289–300.
- [6] Hattori, Masayuki; McEliece, Robert J.(1-CAIT-CS); Solomon, Gustave Subspace subcodes of Reed-Solomon codes. *IEEE Trans. Inform. Theory* 44 (1998), no. 5, 1861–1880.
- [7] Little, John; Schenck, Hal Toric surface codes and Minkowski sums. *SIAM J. Discrete Math.* 20 (2006), no. 4, 999–1014 (electronic).
- [8] Ruano, Diego On the structure of generalized toric codes. *J. Symbolic Comput.* 44 (2009), no. 5, 499–506.
- [9] Ruano, Diego On the parameters of r -dimensional toric codes. *Finite Fields Appl.* 13 (2007), no. 4, 962–976.
- [10] Shibuya, Tomoharu; Matsumoto, Ryutaroh; SAKANIWA, Kohichi. An Improved Bound for the Dimension of Subfield Subcodes .*IEICE TRANS. FUNDAMENTALS*, VOL. E80 A, NO. 5 MAY 1997.
- [11] Stichtenoth, Henning(D-ESSN) On the dimension of subfield subcodes. *IEEE Trans. Inform. Theory* 36 (1990), no. 1, 90–93.
- [12] Stichtenoth, Henning Algebraic function fields and codes. Second edition. *Graduate Texts in Mathematics*, 254. Springer-Verlag, Berlin, 2009. xiv+355 pp. ISBN: 978-3-540-76877-7.